



# Endurecimiento de la red



# INTRODUCCIÓN

Amazon Inspector realiza análisis de todas sus configuraciones de red, como grupos de seguridad, listas de control de acceso de red (ACL de red), tablas de ruta y gateways de Internet, juntas para inferir la accesibilidad. No necesita enviar paquetes a través de la red de nube virtual privada (VPC) o conectarse a los puertos de red de una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Es como un mapeo y reconocimiento de red sin paquetes.

## OBJETIVOS

- Configurar Amazon Inspector.
- Ejecutar una auditoría de red sin agente.
- Investigar los resultados del análisis.
- Actualizar grupos de seguridad.
- Inicie sesión en una estancia del servidor de aplicación usando AWS Systems Manager Session Manager.



# TAREA 1

Para crear un objetivo de evaluación para Amazon Inspector Classic para evaluar, debe comenzar por etiquetar las instancias de EC2 que desea incluir en su objetivo. En esta tarea, etiquetará la instancia de BastionServer.

- En la Consola de administración de AWS, seleccione Services (Servicios) y seleccione EC2.
- En el panel de navegación izquierdo, elija Instances.
- Seleccione la instancia de BastionServer.

The screenshot shows the AWS Management Console interface. On the left, the navigation pane is open, showing 'Instances' under the 'EC2' section. The main content area displays a table of instances. The 'BastionServer' instance is selected, and its details are shown below the table. The instance is in the 'En ejecución' (Running) state.

Name	ID de la instancia	Estado de la instancia	Tipo de instancia	Comprobación de estado	Estado de la instancia	Zona de disponibilidad	DNS de IP pública
AppServer	i-03c6c945a23525afb	Pendiente	t2.micro	-	Ver alarmas	us-west-2a	ec2-54-201...
BastionServer	i-013acff33fd7ae55b	En ejecución	t2.micro	Iniciando	Ver alarmas	us-west-2a	ec2-34-221...

**i-013acff33fd7ae55b (BastionServer)**

**Resumen de instancia**

- ID de la instancia: i-013acff33fd7ae55b (BastionServer)
- Dirección IPv6: -
- Tipo de nombre de anfitrión: -
- Nombre de IP: ip-10-0-1-247.us-west-2.compute.internal
- Responder al nombre DNS de recurso privado: -
- Dirección IPv4 pública: 34.220.100.103 | [dirección abierta](#)
- Estado de la instancia: **En ejecución**
- Nombre DNS de IP privada (solo IPv4): ip-10-0-1-247.us-west-2.compute.internal
- Direcciones IPv4 privadas: 10.0.1.247
- DNS de IPv4 pública: ec2-34-220-100-103.us-west-2.compute.amazonaws.com | [dirección abierta](#)
- Direcciones IP elásticas: -



- Seleccione la pestaña Tags (Etiquetas).
- Seleccione Manage Tags (Administrar etiquetas).
- Seleccionar la pestaña de etiquetas, administrar etiquetas y agregar la información. Seleccione guardar.

**Administrar etiquetas** [Información](#)

Las etiquetas son rótulos personalizados que se asignan a un recurso de AWS. Puede utilizar etiquetas para organizar e identificar las instancias.

Clave	Valor - <i>opcional</i>	
<input type="text" value="Name"/>	<input type="text" value="BastionServer"/>	<button>Eliminar</button>
<input type="text" value="cloudlab"/>	<input type="text" value="c126711a3165679l7344441t1w"/>	<button>Eliminar</button>
<input type="text" value="SecurityScan"/>	<input type="text" value="true"/>	<button>Eliminar</button>

Agregar nueva etiqueta

Puede agregar hasta 47 etiquetas más.

CancelarGuardar



# TAREA 2

En esta tarea, aprenderá a ejecutar una auditoría de red sin agente en sus instancias de EC2 usando Amazon Inspector. Para este laboratorio, usará el paquete de reglas de accesibilidad de red.

- o Seleccionar el servicio Inspector en el apartado de servicios.

The screenshot shows the Amazon Inspector console page. At the top, there's a navigation bar with the AWS logo, 'Servicios', a search bar, and a user profile. The main header area says 'Seguridad, identidad y conformidad' and 'Amazon Inspector administración automatizada y continua de la vulnerabilidad a escala'. Below this, a description states: 'Amazon Inspector es un servicio automatizado de administración de vulnerabilidades que analiza continuamente las cargas de trabajo en busca de vulnerabilidades de software y exposición involuntaria de la red.' To the right, there's a 'Prueba gratuita de 15 días' section with a 'Comenzar' button. Below the main header, there's a 'Cómo funciona' section with a diagram showing the workflow: 'Amazon Inspector' (Discover and scan) -> 'Escanear Amazon Inspector' (Analyze) -> 'Generar informe' (Generate report) -> 'Compartir informe' (Share report). The diagram also shows 'Amazon Inspector' interacting with 'AWS Security Hub', 'Amazon EventBridge', 'Amazon ECR', and 'AWS IAM'. On the right side of the console, there are sections for 'Precios' (Pricing), 'Más información' (More information), and 'Documentación' (Documentation).

- o Seleccione Switch to Inspector Classic (Cambiar a Inspector Classic).



aws Servicios Q Buscar [Alt+S] Oregón voclabs/user3386630=Joseph\_Julios @ 0247-7296-4763

## Amazon Inspector

Amazon Inspector le permite analizar el comportamiento de sus recursos de AWS y le ayuda a identificar posibles problemas de seguridad.

[Empezar](#)

### Instalar

Instale el agente de AWS en las instancias EC2.

[Más información](#)

### Ejecutar

Ejecute una evaluación del objetivo de evaluación.

[Más información](#)

### Analizar

Examine los hallazgos y solucione los problemas de seguridad.

[Más información](#)

[Documentación y soporte de Amazon Inspector](#)

CloudShell Comentarios © 2024, Amazon Web Services, Inc. o sus filiales. Privacidad Términos Preferencias de cookies

- o Seleccione Get Started.
- o Seleccione Advanced setup.
- o Configurar la sección de Definir un objetivo de evaluación.

aws Servicios Q Buscar [Alt+S] Oregón voclabs/user3386630=Joseph\_Julios @ 0247-7296-4763

## Introducción a Amazon Inspector

**Step 1: Define an assessment target**

Step 2: Define an assessment template

Step 3: Review

### Definir un objetivo de evaluación

Un objetivo de evaluación representa una colección de recursos de AWS que le ayudan a lograr sus objetivos empresariales. [Más información.](#)

**Nombre\***

**All Instances** ☐ Include all EC2 instances in this AWS account and region.

**Note:** The limit on the maximum number of agents that can be included in an assessment run applies. [Learn more](#)

**Etiquetas\***

Clave	Valor
SecurityScan	<input type="text" value="true"/>
Añada una clave nueva	<input type="text"/>

**Install Agents** ☐ Install the Amazon Inspector Agent on all EC2 instances in this assessment target.

To use this option, make sure that your EC2 instances have the SSM Agent installed and an IAM role that allows Run Command. [Learn more](#)

**\*Obligatorio**

[Cancelar](#) [Vista previa](#) [Siguiente](#)

CloudShell Comentarios © 2024, Amazon Web Services, Inc. o sus filiales. Privacidad Términos Preferencias de cookies



## ○ Configurar la sección de Definir una plantilla de evaluación.

**Introducción a Amazon Inspector**

**Step 1: Define an assessment target**  
**Step 2: Define an assessment template**  
**Step 3: Review**

### Definir una plantilla de evaluación

Una plantilla de evaluación le permite especificar diversas propiedades para una ejecución de evaluación, incluidos los paquetes de reglas, la duración, las notificaciones SNS y cómo etiquetar cualquier hallazgo. [Más información.](#)

**Nombre\***

**Paquetes de reglas\***  ×

Amazon Inspector realiza las evaluaciones del objetivo de evaluación especificadas en los paquetes de reglas seleccionados. [Más información.](#)

**Duración\***

La duración predeterminada de la plantilla de evaluación de Amazon Inspector es de 1 hora. Puede modificar la duración, pero tenga en cuenta que las plantillas de evaluación con duraciones más largas pueden proporcionar conjuntos de hallazgos más completos.

**Assessment Schedule** ☐ Set up recurring assessment runs once every  days. **The first run starts on create.** [Más información](#)

\*Obligatorio

[Cancelar](#) [Anterior](#) [Siguiente](#)

## ○ Verificar el estado del análisis.

**Panel**  
Objetivos de evaluación  
Plantillas de evaluación  
**Ejecuciones de evaluación**  
Hallazgos  
[Switch to Inspector V2](#)

### Amazon Inspector - Ejecuciones de evaluación

Una ejecución de evaluación es una instancia de una plantilla de evaluación que se ejecuta para analizar el comportamiento del objetivo de evaluación. [Más información.](#)

**Ejecutar - Assessment-Template-Network - 2024-08-21T00:28:03.710Z** ×

Amazon Inspector assessed **Network-Audit** for 30 seconds.

[Actualizar](#) [Cerrar](#)

**Evaluación - Ejecutar - Assessment-Template-Network - 2024-08-21T00:28:03.710Z**

**ARN** `arn:aws:inspector:us-west-2:024772964763:target/0-Jngum7Ma/template/0-xPKowccP/run/0-jwFdtBFw`

**Inicio** Today at 7:28 PM (GMT-5) (3 minutes ago)

**Fin** Today at 7:28 PM (GMT-5) (2 minutes ago)

**Nombre del objetivo** [Network-Audit](#)

**Nombre de la plantilla** [Assessment-Template-Network](#)

**Paquetes de reglas** [Network Reachability-1.1](#)

**Duración** 15 Minutos

[Descargar informe](#)



- Cuando el estado cambie a Analysis complete, seleccione Findings en el panel de navegación.

Introducing the new Amazon Inspector

The new Amazon Inspector is a completely rearchitected version of the existing Inspector Classic. The new Inspector is an automated vulnerability management service that continually scans your EC2 and Container workloads for software vulnerabilities and unintended network exposure. [Más información](#) [Start your free trial](#)

## Amazon Inspector - Hallazgos

Los hallazgos son posibles problemas de seguridad detectados por Amazon Inspector durante la ejecución de una evaluación del objetivo de evaluación especificado. [Más información](#).

Filtros: [{"assessmentRunArns":["arn:aws:inspector:us-west-2:024772964763:target/0-jngum7Ma/template/0-xPKowccP/run/0-jwFdtBFw"]}]

[Añadir/Editar atributos](#) Última actualización: 2024/8/20 7:31:53 p. m. (hace 0 min.)

Filtro

	Gravedad	Fecha	Hallazgo	Objetivo	Plantilla	Paquete de reglas
<input type="checkbox"/>	Alta	Today at 7:2...	On instance i-013acff33fd7ae55b, TCP port 23 whi...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Media	Today at 7:2...	On instance i-013acff33fd7ae55b, TCP port 22 whi...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Informativa	Today at 7:2...	Aggregate network exposure: On instance i-013acf...	Network-Audit	Assessment-Temp...	Network Reachability-1.1

Máximo de registros por página: 25

\* actualice el navegador para reflejar el cambio

CloudShell Comentarios

© 2024, Amazon Web Services, Inc. o sus filiales. Privacidad Términos Preferencias de cookies





## TAREA 3

Los hallazgos que esas reglas generan muestran si sus puertos son accesibles desde Internet mediante un gateway de Internet (incluidas instancias detrás de equilibradores de carga de aplicación o equilibradores de carga clásicos), una interconexión de VPC o una red privada virtual (VPN) mediante un gateway virtual. Estos hallazgos también destacan las configuraciones que permiten potenciales accesos maliciosos, como grupos de seguridad, ACL y gateways de Internet mal administrados.

- Revisar el hallazgo de alta severidad. Debería poder ver los siguientes detalles clave.

The screenshot shows the AWS Inspector console interface. At the top, there's a navigation bar with the AWS logo, 'Servicios', a search bar, and a user profile. The main content area displays details for a specific finding. The finding is titled 'Network-Audit' and is associated with the template 'Assessment-Template-Network'. It was executed on '2024-08-21T00:28:03.710Z'. The finding is of 'High' severity and is described as 'On instance i-013acff33fd7ae55b, TCP port 23 which is associated with 'Telnet' is reachable from the internet'. The description further explains that the instance is in VPC vpc-085853d06bb3a0afa and has an attached ENI eni-03026d27eef20ee8e which uses network ACL acl-081d0ca0bc7acefd6. The port is reachable from the internet through Security Group sg-04184a80be1da912f and IGW igw-0ecb89219329a4605.

ARN	arn:aws:inspector:us-west-2:024772964763:target/0-Jngum7Ma/template/0-xPKowccP/run/0-jwFdtBFw/finding/0-T60TVcHL
Nombre de la ejecución	Ejecutar - Assessment-Template-Network - 2024-08-21T00:28:03.710Z
Nombre del objetivo	Network-Audit
Nombre de la plantilla	Assessment-Template-Network
Inicio	Today at 7:28 PM (GMT-5) (6 minutes ago)
Fin	Today at 7:28 PM (GMT-5) (5 minutes ago)
Estado	Análisis finalizado
Paquete de reglas	Network Reachability-1.1
ID de agente de AWS	i-013acff33fd7ae55b
Hallazgo	On instance i-013acff33fd7ae55b, TCP port 23 which is associated with 'Telnet' is reachable from the internet
Gravedad	High
Descripción	On this instance, TCP port 23, which is associated with Telnet, is reachable from the internet. You can install the Inspector agent on this instance and re-run the assessment to check for any process listening on this port. The Instance i-013acff33fd7ae55b is located in VPC vpc-085853d06bb3a0afa and has an attached ENI eni-03026d27eef20ee8e which uses network ACL acl-081d0ca0bc7acefd6. The port is reachable from the internet through Security Group sg-04184a80be1da912f and IGW igw-0ecb89219329a4605



- o Revisar los hallazgos de severidad media y analizar los detalles.

aws

Servicios

Q Buscar

[Alt+S]

Oregón

voclabs/user3386630-Joseph\_Julios @ 0247-7296-4763

ARN

arn:aws:inspector:us-west-2:024772964763:target/0-Jngum7Ma/template/0-xPKowccP/run/0-jwFdtBFw/finding/0-Gp9l1C0d

Nombre de la ejecución

Ejecutar - Assessment-Template-Network - 2024-08-21T00:28:03.710Z

Nombre del objetivo

Network-Audit

Nombre de la plantilla

Assessment-Template-Network

Inicio

Today at 7:28 PM (GMT-5) (7 minutes ago)

Fin

Today at 7:28 PM (GMT-5) (6 minutes ago)

Estado

Analisis finalizado

Paquete de reglas

Network Reachability-1.1

ID de agente de AWS

i-013acff33fd7ae55b

Hallazgo

On instance i-013acff33fd7ae55b, TCP port 22 which is associated with 'SSH' is reachable from the internet

Gravedad

Medium ⓘ

Descripción

On this instance, TCP port 22, which is associated with SSH, is reachable from the internet. You can install the Inspector agent on this instance and re-run the assessment to check for any process listening on this port. The instance i-013acff33fd7ae55b is located in VPC vpc-085853d06bb3a0afa and has an attached ENI eni-03026d27eef20ee8e which uses network ACL acl-081d0ca0bc7acefd6. The port is reachable from the internet through Security Group sg-04184a80be1da912f and IGW igw-0ecb89219329a4605

Recomendación

You can edit the Security Group sg-04184a80be1da912f to remove access from the internet on port 22

Show Details

CloudShell

Comentarios

© 2024, Amazon Web Services, Inc. o sus filiales.

Privacidad

Términos

Preferencias de cookies



# TAREA 4

En esta tarea, verá algunas opciones de corrección para los hallazgos de seguridad que Amazon Inspector detectó. La primera opción muestra cómo bloquear el puerto 22 para direcciones IP específicas.

- Revisar los detalles del hallazgo de alta severidad.
- Seleccionar el enlace para el grupo de seguridad. Los enlaces deben ser similares al siguiente ejemplo: sg-0b2dc685cd6e6e706.
- Editar las reglas de entrada.

The screenshot shows the AWS Management Console interface for editing inbound rules of a security group. The breadcrumb trail is: EC2 > Grupos de seguridad > sg-04184a80be1da912f > Editar reglas de entrada. The page title is 'Editar reglas de entrada' with an 'Información' link. A note states: 'Las reglas de entrada controlan el tráfico entrante que puede llegar a la instancia.' The main section is titled 'Reglas de entrada' with an 'Información' link. It contains a table with the following columns: 'ID de la regla del grupo de seguridad', 'Tipo', 'Protocolo', 'Intervalo de puertos', 'Origen', and 'Descripción: opcional'. The first row shows a rule with ID 'sgr-090de6252b2161c13', Type 'SSH', Protocol 'TCP', Port range '22', and Origin 'Mi IP'. Below the table, there is an 'Agregar regla' button. At the bottom right, there are three buttons: 'Cancelar', 'Previsualizar los cambios', and 'Guardar reglas'.

ID de la regla del grupo de seguridad	Tipo	Protocolo	Intervalo de puertos	Origen	Descripción: opcional
sgr-090de6252b2161c13	SSH	TCP	22	Mi IP	

Buttons: Agregar regla, Cancelar, Previsualizar los cambios, Guardar reglas



- Ejecutar la plantilla de evaluación Assessment-Template-Network.

Introducing the new Amazon Inspector

The new Amazon Inspector is a completely rearchitected version of the existing Inspector Classic. The new Inspector is an automated vulnerability management service that continually scans your EC2 and Container workloads for software vulnerabilities and unintended network exposure. [Más información](#) [Start your free trial](#)

## Amazon Inspector - Plantillas de evaluación

Una plantilla de evaluación le permite especificar diversas propiedades para una ejecución de evaluación, incluidos los paquetes de reglas, la duración, las notificaciones SNS y cómo etiquetar cualquier hallazgo. [Más información](#).

[Crear](#) [Ejecutar](#) [Eliminar](#) [Clonar](#) [Crear eventos de evaluación](#)

Última actualización: 2024/8/20 7:42:29 p. m. (hace 0 min.)

Filtro 1 seleccionada(s) Mostrando 1-1 de 1

	Nombre	Duración	Nombre del objetivo	Última ejecución	Todas l...
<input checked="" type="checkbox"/>	Assessment-Template-Network	15 Minutos	Network-Audit	Análisis finalizado	1

Máximo de registros por página: 25

\* actualice el navegador para reflejar el cambio

- Seleccionar Ejecuciones de evaluación.
- Revisar los hallazgos y seleccionarlos según fecha.

Introducing the new Amazon Inspector

The new Amazon Inspector is a completely rearchitected version of the existing Inspector Classic. The new Inspector is an automated vulnerability management service that continually scans your EC2 and Container workloads for software vulnerabilities and unintended network exposure. [Más información](#) [Start your free trial](#)

## Amazon Inspector - Hallazgos

Los hallazgos son posibles problemas de seguridad detectados por Amazon Inspector durante la ejecución de una evaluación del objetivo de evaluación especificado. [Más información](#).

Filtros: ["assessmentRunArns":["arn:aws:inspector:us-west-2:024772964763:target/0-xPkcwcp/run/0-B2YgSx83"]]

[Añadir/Editar atributos](#)

Última actualización: 2024/8/20 7:47:03 p. m. (hace 0 min.)

Filtro Mostrando 1-2 de 2

	Gravedad	Fecha	Hallazgo	Objetivo	Plantilla	Paquete de reglas
<input type="checkbox"/>	Media	Today at 7:4...	On Instance I-013acff33fd7ae55b, TCP port 22 whi...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Informativa	Today at 7:4...	Aggregate network exposure: On instance I-013acf...	Network-Audit	Assessment-Temp...	Network Reachability-1.1

Máximo de registros por página: 25

\* actualice el navegador para reflejar el cambio



# TAREA 5

En esta tarea, reemplazó la instancia de BastionServer, que usaba principalmente SSH para conectarse a AppServer dentro de la subred privada. En su lugar, usted usa Session Manager mediante Systems Manager.

- Ubicarse en el servicio EC2 de AWS, en el apartado de grupo de seguridad.
- Editar reglas de entrada para BastionServerSG, eliminar la regla de entrada de SSH.

aws Servicios  [Alt+S] Oregón voclabs/user3386630=Joseph\_Julios @ 0247-7296-4763

[EC2](#) > [Grupos de seguridad](#) > [sg-04184a80be1da912f - c126711a3165679l7344441t1w024772964763-BastionSG-Uf4Hhf2l3oj8](#) > Editar reglas de entrada

## Editar reglas de entrada [Información](#)

Las reglas de entrada controlan el tráfico entrante que puede llegar a la instancia.

**Reglas de entrada** [Información](#)

Este grupo de seguridad no tiene reglas de entrada.

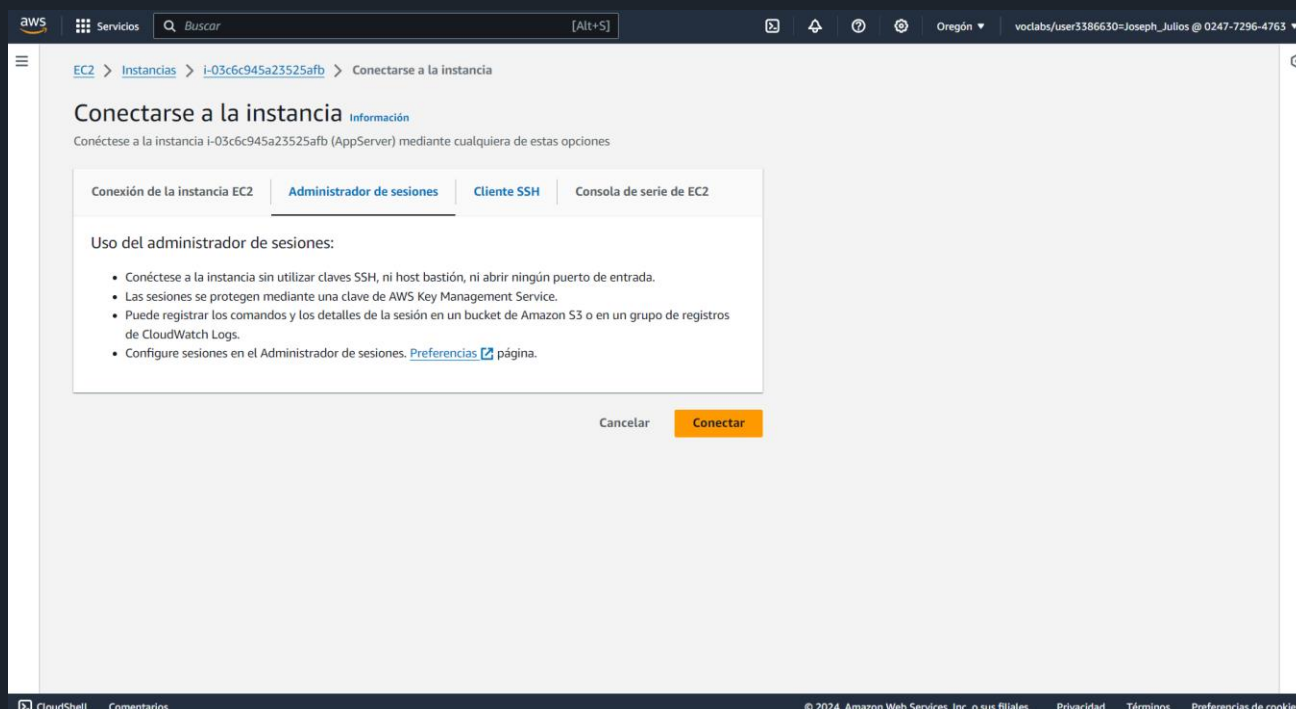
[Agregar regla](#)

[Cancelar](#) [Previsualizar los cambios](#) [Guardar reglas](#)

[CloudShell](#) [Comentarios](#) © 2024, Amazon Web Services, Inc. o sus filiales. [Privacidad](#) [Términos](#) [Preferencias de cookies](#)



- Detener instancia BastionServer.
- Conectarse mediante Session Manager a App Server.



- Análisis final, ejecutar evaluación y revisar los detalles de los hallazgos.

ID de sesión: user3386630=Joseph\_Julios-cqfогc6mc7kqwwrhwatcaky2he

ID de instancia: i-03c6c945a23525afb

```
sh-4.2$ cd ~
sh-4.2$ pwd
/home/ssm-user
sh-4.2$
```

- Vaya a la pestaña del navegador que tiene Amazon Inspector abierto.



- En el panel de navegación izquierdo, elija Assessment runs (Ejecuciones de evaluación).
- Seleccione la casilla para la evaluación ejecutada anteriormente y luego seleccione Run (Ejecutar).
- Espere que Status (Estado) muestre Analysis complete (Análisis completo) y seleccione para expandir los detalles de la ejecución de evaluación más reciente.
- Compruebe que no haya ningún Hallazgo.

The screenshot shows the AWS Security Hub console interface. At the top, there's a navigation bar with the AWS logo, 'Servicios', a search bar, and user information. Below this, a table lists assessment runs. The selected run is 'Assessment-Template-Network' with a status of 'Análisis finalizado' (Analysis complete). The details panel for this run shows the following information:

- ARN:** arn:aws:inspector:us-west-2:024772964763:target/0-Jngum7Ma/template/0-xPKowccP/run/0-5s4a2Koi
- Inicio:** Today at 7:56 PM (GMT-5) (a few seconds ago)
- Fin:** Today at 7:56 PM (GMT-5) (a few seconds ago)
- Nombre del objetivo:** Network-Audit
- Nombre de la plantilla:** Assessment-Template-Network
- Paquetes de reglas:** Network Reachability-1.1
- Duración:** 15 Minutos
- Estado:** Análisis finalizado
- Hallazgos:** 0

At the bottom of the details panel, there are buttons for 'Mostrar los agentes de AWS' and 'Mostrar el estado'. The table at the bottom shows the run is completed with 2 findings (0 high, 2 medium, 0 low).